University of Wollongong

Research Online

Faculty of Informatics - Papers (Archive)

Faculty of Engineering and Information Sciences

1987

Constructing Hadamard matrices via orthogonal designs

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Follow this and additional works at: https://ro.uow.edu.au/infopapers

Part of the Physical Sciences and Mathematics Commons

Recommended Citation

Seberry, Jennifer: Constructing Hadamard matrices via orthogonal designs 1987.
https://ro.uow.edu.au/infopapers/1027

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

Constructing Hadamard matrices via orthogonal designs

Abstract

Orthogonal designs were created to give a unifying approach to the construction of Hadamard matrices. Recent work has been concerned with Hadamard matrices of order 2tpq, where t ≤ 5 and one of p and q is small. This paper obtains many new constructions for Hadamard matrices of such orders and works toward a more general construction theory.

Disciplines

Physical Sciences and Mathematics

Publication Details

Seberry, J, Constructing Hadamard matrices via orthogonal designs, Congressus Numerantium, 57, 1987, 299-302.

This journal article is available at Research Online: https://ro.uow.edu.au/infopapers/1027

CONSTRUCTING HADAMARD MATRICES VIA ORTHOGONAL DESIGNS

Jennifer Seberry
Department of Computer Science
University of Sydney
N.S.W., 2006, Australia

Abstract. Orthogonal designs were created to give a unifying approach to the construction of Hadamard matrices. Recent work has been concerned with Hadamard matrices of order $2^t pq$, where $t \leq 5$ and one of p and q is small. This paper obtains many new constructions for Hadamard matrices of such orders and works toward a more general construction theory.

1. Introduction

Let $A = [a_{ij}]$ be a matrix of order n with $a_{ij} \in \{0,1,-1\}$. A is called a *weighing matrix* of weight p and order n if $AA^T = A^TA = pI_n$, where I_n denotes the identity matrix of order n. Such a matrix is denoted by W(n,p). If squaring all its entries gives the incidence matrix of an SBIBD, then W is called a balanced weighing matrix.

An *orthogonal design* (OD)A of order n and type $(s_1,s_2, \ldots, s_t)$ on the commuting variables $(\pm x_1, \ldots ,\pm x_k,0)$ is a square matrix of order n with entries $\pm x_k$ or 0 and with $|x_k|$ occurring s_k times in each row and column such that the rows are pairwise orthogonal. In other words,

$$AA^T = (s_1x_1{}^2 + \ldots + s_tx_t{}^2)I_n.$$

This is denoted by $OD(n;s_1,s_2, \ldots ,s_t)$.

An *Hadamard matrix* , $A = [a_{ij}]$, is either an OD(n;n) or a W(n,n), that is, it is a square matrix of order n with entries $a_{ij} \in \{1,-1\}$ which satisfies

$$AA^T = A^TA = nI_n.$$

2. Constructions

LEMMA 1. *Suppose there is an* OD(p+1;1,p) *and a conference matrix of order* p+3. *Then there is an Hadamard matrix of order* 2(p+1)(p+2) *(divisible by 8).*

Proof. The conference matrix has symmetric core N such that

$$(N+I)^2 + (N - I)^2 = 2(p+3)I - 2J.$$

Use the OD to form an OD (2(p+1);1,1,p,p); then replace its variables by the suitable matrices of order p+2: J, J - 2I, N+I, N - I. Now

$$J^2 + (J-2I)^2 + p\,(N+I)^2 + p\,(N-I)^2$$

$$=(p+2)J + 4I + (p-2)J + 2p\,(p+3)I - 2pJ$$

$$=2(p+1)(p+2)I, \qquad \text{and we have the result.}$$

CONGRESSUS NUMERANTIUM **57**(1987), pp.299-302

LEMMA 2. *Suppose there exists an* OD(2(p+1); 2, 2p) *and a symmetric Hadamard matrix of order* p+3. *Then there is an Hadamard matrix of order* 4(p+1)(p+2).

Proof. The symmetric Hadamard matrix has symmetric core B of order p+2 satisfying

$$B^2 = (p+3)I - J.$$

Use the $OD\,(2(p+1);2,2p)$ to form an $OD\,(4(p+1);2,2,4p)$. Replace the variables by the suitable matrices of order $p+2$: J, $J-2I$, B. Now

$$\begin{aligned}&2J^2 + 2(J-2I)^2 + 4pB^2\\ &= 2(p+2)J + 2(4I + (p-2)J) + 4p\,((p+3)I - J)\\ &= 4(p+1)(p+2)I,\end{aligned}$$

and we have the result.

Example. A symmetric conference matrix of order 102 exists. Hence an $OD\,(204;2;202)$ exists. A symmetric Hadamard matrix of order 104 exists. Hence we have an Hadamard matrix of order 8.51.103 (which was previously known) even though an Hadamard matrix of order 4.103 is not yet known.

LEMMA 3. *Suppose there is an* OD(3r+1;1,3r) *and a symmetric Hadamard matrix of order* 4r+4 *with core B of order* 4r+3. *Then there is an Hadamard matrix of order* 4(3r+1)(4r+3) *(divisible by 16).*

Proof. The symmetric core satisfies

$$B^2 = (4r+4)I - J.$$

Use the OD(3r+1;1,3r) to form an OD(4(3r+1);1,2,12r+1). Replace the variables by the suitable matrices of order 4r+3: J, J - 2I, B. Now

$$\begin{aligned}&J^2 + 2(J - 2I)^2 + (12r+1)B^2\\ &= (4r+3)J + 2(4I + (4r-1)J) + (12r+1)((4r+4)I - J)\\ &= 4(3r+1)(4r+3)I,\end{aligned}$$

and we have the result.

Example 1. A small interesting example is for r=13 which gives an Hadamrad matrix of order 4(40)55 = 16 × 275. An Hadamard matrix of order 4 × 275 is already known.

Example 2. An Hadamard matrix of order 4.103 is not yet known but an OD(76;1,75) exists and a symmetric Hadamard matrix of order 104. So there is an Hadamard matrix of order 16.19.103. The Hadamard matrix of order $16 \cdot 19 \cdot 103$ is known but matrices are not yet known for orders $4 \cdot 19 \cdot 103$ or $8 \cdot 19 \cdot 103$.

LEMMA 4. Let v be a prime, and Q *be a cyclic (1,-1) incidence matrix of a* (v,k,λ).*Suppose an* $OD\,(s(t+1);s,st)$ *exists. Then there exists an Hadamard matrix of order* $s(t+1)$ v or $2s(t+1)$v *according as* v $\equiv 3 (mod 4)$ *or* $1 (mod 4)$.

Proof. Q satisfies

$$QQ^T = 4(k-\lambda)I + (v-4(k-\lambda))J = 4(k-\lambda I + tJ.$$

Since v is prime,there exists a b ack circulant BR ($if v \equiv 3 (mod 4)$) which satisfies

$$(BR)^2 = (v+1)I - J \qquad \text{(a)}$$

$$((X+I)R)^2+((X-I)R)^2 = 2(v+1)I-2J, X\ T=X. \qquad \text{(b)}$$

Thus we use the suitable matrices:

(a) Q, BR in the $OD\,(s\,(t+1);s,st)$ for $v \equiv 3(mod 4)$ and note

$$sQ^2+st\,(BR)^2 = 4s\,(k-\lambda)I+stJ+st\,(v+1)I-stJ$$

$$= sv\,(t+1)I;$$

(b) Q, $(X+I)R$, $(X-I)R$ in the $OD\,(2s\,(t+1);2s,st,st)$ for $v \equiv 1 \pmod 4$ and note

$$2sQ^2 + st\,(XR+R)^2 + st\,(XR-R)^2 = 2sv\,(t+1)I.$$

This gives the result.

v	OD required	E	(v,k,λ)-design	(1,-1) matrix	Hadamard Matrix constructed	E
31	OD(12;1,11)	√	(31,6,1)	20I+11J	12.31 = 4.3.31	√
31	OD(36;3,33)	√	(31,6,1)	20I+11J	36.31 = 4.9.31	√
31	OD(12t;t,11t)	?	(31,6,1)	20I+11J	12t.31 = 4.3t.31	?
31	OD(24;1,1,11,11)	√	(31,6,1)	20I+11J	24.31 = 8.3.31	√
31	OD(12h;h,11h)	?h	(31,6,1)	20I+11J	12h.31†	??
31	OD(24n;n,n,11n,11n)	?	(31,6,1)	20I+11J	24n.31††	??
37	OD(20;2,9,9)	√	(37,9,2)	28I+9J	20.37=4.185	√
57	OD(60;2,29,29)	?	(57,8,1)	28I+29J		?
57	OD(120;4,58,58)	√	(57,8,1)	28I+29J	120.57=8.15.57	√
73	OD(84;2,41,41)	?	(73,9,1)	32I+41J		?
73	OD(168;4,82,82)	√	(73,9,1)	32I+41J	168.73=8.21.73	√
307	OD(308;1,307)	√	(307,18,1)	68I+307J	308.307=4.77.307	√
121	OD(28;2,13,13)	√	(121,40,13)	108I+13J	28.121=4.7.121	√
1093	OD(244;2,121,121)	?	(1093,364,121)	972I+121J		?
1093	OD(488;4,242,242)	√	(1093,364,121)	972I+121J	488.1093=8.61.1093	√
197	OD(100;2,49,49)	?	(197,49,12)	146I+49J		?
197	OD(200;4,98,98)	√	(197,49,12)	146I+49J	200.197=8.25.197	√

† h is the order of an Hadamard matrix.

†† n is the order of a conference matrix.

We can find more results using the back circulant incidence matrices,Q, of (v, k, λ) designs, v prime, which satisfy

$Q^2 = 4(k-\lambda)I + tJ$, where $t = v - 4(k-\lambda)$, (*)

the circulant (1,-1)- incidence matrices B or $X+I, X-I$ of the (v,½(v − 1) , ¼ (v − 3)) difference set or 2 − {v;½ (v − 1);½ (v − 3)} supplementary difference sets, according as v ≡ 3(mod4) or v ≡ 1(mod4) and which satisfy

$$BB^T = (v+1)I - J, v \equiv 3(mod\,4) \qquad (**)$$

and

$$(X+I)^2 + (X-I)^2 = 2(v+1)I - 2J,\ X^T = X, v \equiv 1\ (mod\,4) \qquad (***)$$

In most cases the power of the theorem is limited by the knowledge of the existence of orthogonal designs.

THEOREM 5 *Let* v *be a prime. Let* Q *be the back-circulant* (1,-1) *incidence matrix of a* (v,k,λ)*design* $(k\neq\frac{1}{2}(v\pm 1))$, t *as above. Suppose there exists an* $OD(4n;a,b,4n-a-b)$. *Then*

(i) *for* $v\equiv 3(mod 4)$ *there exist Hadamard matrices of order* $4nv$ *when* $a(v+1)+b(t+1)=4n$;

(ii) *for* $v\equiv 1(mod 4)$ *there exist Hadamard matrices of order* $8nv$ *when* $a(v+1)+b(t+1)=4n$.

Proof. Use the suitable matrices Q,J,B, in (i) and $Q,J,X+I,X-I$, in the $OD(8n;2a,2b,4n-a-b,4n-a-b)$ in (ii).

Order 13 is a special case for there is a back circulant (1,-1)matrix Q of a (13, 4, 1) design. So that we have

COROLLARY 6. *Suppose there exists an* OD $(4t:2t,t,t)$ *design. Then there exists an Hadamard matrix of order* $4t.13$. *Such an* OD *exists for infinitely many t*

Proof. Replace the variables of the $OD(4t;2t,t,t,)$ by $Q,X+I,X-I$.

Example. Let $v=31$ and Q be obtained from the (31,6,1) design;so $Q^2=20I+11J$.

Now suppose an $OD(76;1,2,73)$ exists;then,using the suitable matrices Q,J,B,we get an Hadamard matrix of order 4.19.31.

Using the $OD(56;1,2,53)$ and the suitable matrices J,Q,B,we obtain the Hadamard matrix of order 8.7.31.

Many more results could follow;we tabulate some of the possibilities:

OD that needs to exist	Known or N.E?	Suitable matrices	Hadamard matrix
OD(56;1,2,53)	√	J,Q,B	8.7.31
OD(76;1,2,73)	?	Q,J,B	4.19.31
OD(68;1,3,64)	?	J,Q,B	4.17.31
OD(108;1,3,104)	?	Q,J,B	4.27.31
OD(80;1,4,75)	√	J,Q,B	16.5.31
OD(140;1,4,135)	?	Q,J,B	4.35.31
OD(100;2,3,95)	?	J,Q,B	4.25.31
OD(120;2,3,115)	?	Q,J,B	8.15.31
OD(124;2,5,117)	?	J,Q,B	4.31^2
OD(184;2,5,177)	?	Q,J,B	8.23.31
OD(144;3,4,137)	?	J,Q,B	16.9.31
OD(164;3,4,157)	?	Q,J,B	4.31.41

References

A.V.Geramita and Jennifer Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices,* Marcel Dekker, New York-Basel, 1979.

W.D.Wallis, Anne Penfold Street, Jennifer Seberry Wallis, *Combinatorics: Room Squares, sum free sets, Hadamard Matrices,* Lecture Notes in Mathematics, Vol. 292, Springer Verlag, Berlin-Heidelberg- New York, 1972.